Cybersecurity of Development Environments

May 2020

Megan Fisher

412TENG/JT4

DISTRIBUTION STATEMENT A - Approved for public release; distribution is unlimited.
412TW-PA-21209

412TENG CTTs

- Airborne Instrumentation
- TSPI
- Development Environments
- Data Centers
- More to follow!

Development Environments

- Critical to advancing technology
- Must be agile to accomplish their mission
- Traditional security does not always work

Why a Cyber table top?

- Buy-in
- Inexpensive
- Flexible
- Road Map

CTT-LITE

- Low Impact To Execute
- Reduced Scope

- Planning: 3 months
- Execution: 2 days

Scope

- **Goal: understand the risk development environments pose to mission systems**

- **Out of Scope:**
  - **Working remotely**
  - **Connections to cloud environments**

System

- **Fabricated development environment:**

Set of computers and equipment (hardware and software) that generates knowledge and products used to operate and maintain mission systems (instructions, software source code, drawings, designs, hardware, procedures, configuration files etc…)

Cyber Mission

- **Cyber Team:**
  - **412TENG Cybersecurity Engineering Support Team (CSEST)**
  - **47th CTS**
  - **Intel**

- **Attacks (40) were divided into 3 missions:**
  - **Gain logical access**
  - **Disrupt the development environment (16)**
  - **Corrupt, destroy, modify or exfiltrate product (12)**

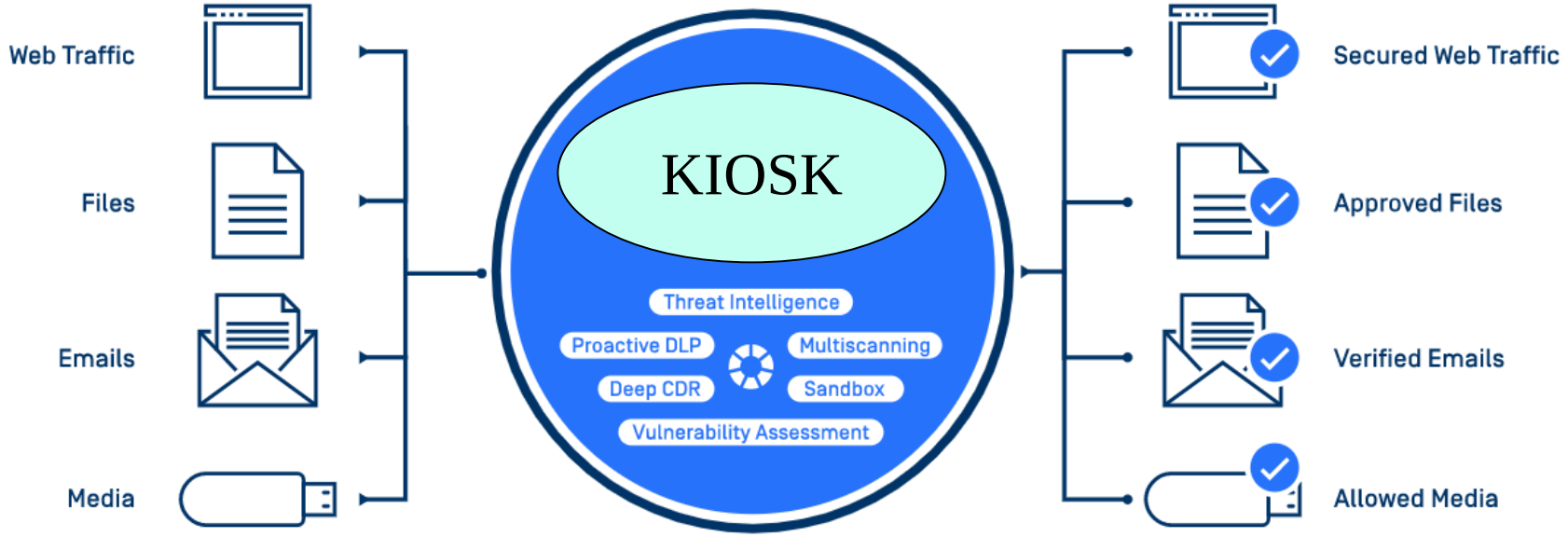
Risk Matrix

- 30 total attacks
- 13 with high likelihood and impact

Number of Attacks at Given Coordinates

Likelihood of Successful Cyber Attack				
4	4	2	3	1
1	1	1		2
		1	1	5
1			1	1
		1		

Impact Resulting from Cyber Attack

Findings

- **Boundary Protections**
  - **Physical security**
  - **Kiosk**
- **Back-ups**